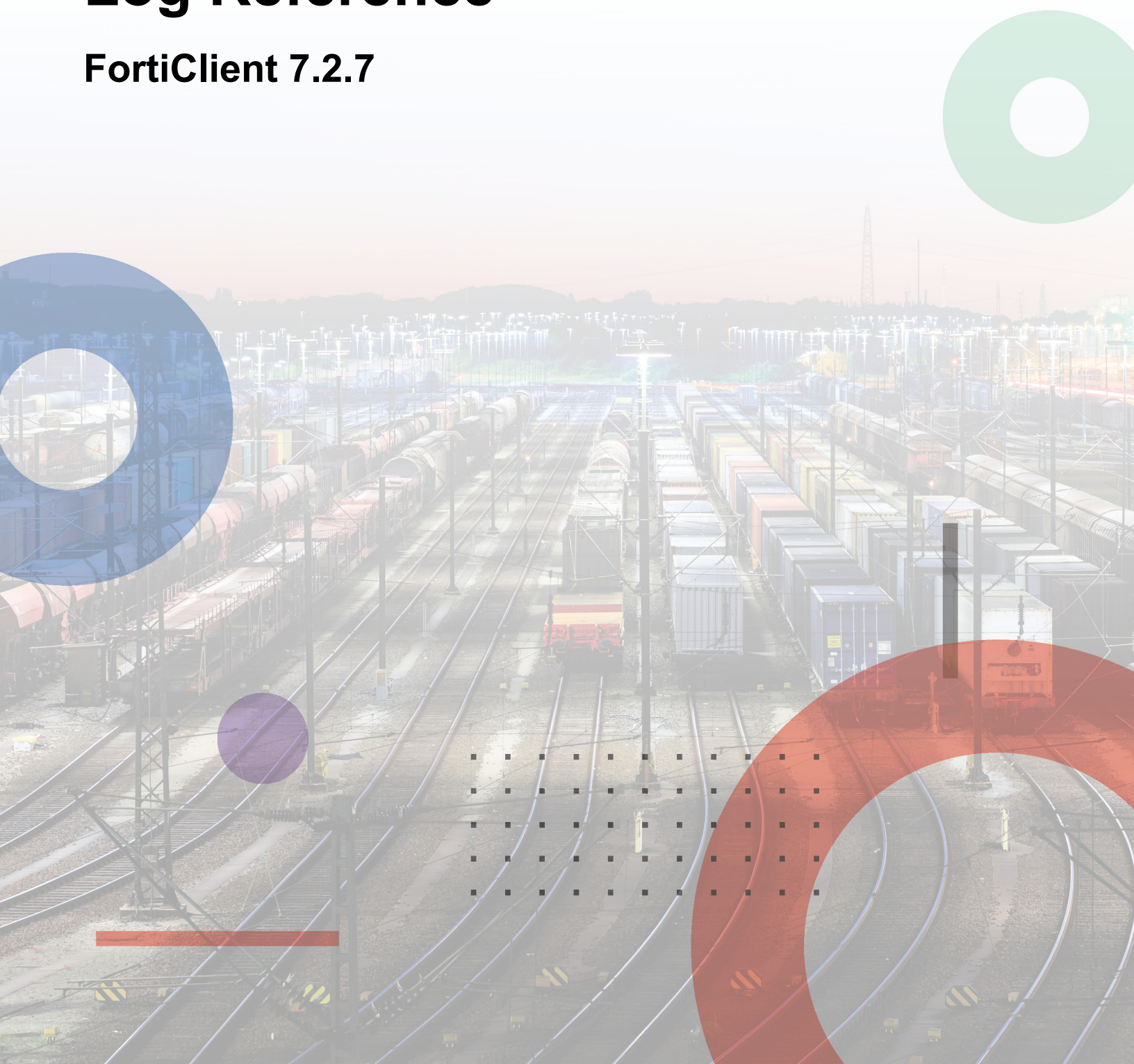
Log Reference

FortiClient 7.2.7



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 12, 2024
FortiClient 7.2.7 Log Reference
04-727-877833-20241212

TABLE OF CONTENTS

Change log

Date	Change description
2024-12-12	Initial release.

Introduction

This document provides information about all the log messages applicable to FortiClient 7.2.7. The logs are intended for administrators to use as reference for more information about a specific log entry and message that FortiClient generated.

FortiClient has the following log types:

- Security event
- System event
- Traffic

This document contains the following information:

- Windows on page 6: fields that apply to FortiClient (Windows) logs
- Linux on page 15: fields that apply to FortiClient (Linux) logs

Windows

This section contains the following information for FortiClient (Windows):

- Mandatory fields on page 6: fields that are mandatory to all FortiClient (Windows) logs.
- Log fields by type on page 7: fields that only apply to security event logs.
- Log message by type on page 10: lists each possible log message, sorted by log type and subtype.

Mandatory fields

Log Field Name	Description	Data Type
date	date	string
time	time	string
logver	log protocol version	int
id	log id	int
type	Traffic, Security Event or System Event	string
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string
eventtype	type of event	enumeration string
level	log level	enumeration string
uid	FortiClient unique ID	string
devid	device ID	string
hostname	host name of local machine	string
pcdomain	domain name of local machine	string
deviceip	device IP address	string
devicemac	device MAC address	string
vd	vdom	string
fctver	FCT version	string
fgtserial	FGT serial number	string
emsserial	EMS serial number	string
usingpolicy	current policy name	string

Log Field Name	Description	Data Type
os	operating system	string
user	current logged on user	string
msg	description of this log	string

Log fields by type

securityevent

Log Field Name	Description	Data Type	Length
action	block or monitor	string	32
file	file location	string	256
virus	virus name	string	512
sigid	signature id	string	260
from	email from	string	128
to	email to	string	512
service	network protocol	string	64
vpn	vpn tunnel name	string	32
filesize	file size	int	20
checksum	file crc32 checksum	int	20
detectedby	the security feature that detected virus	enumeration string	64
detectedin	where the virus is detected	enumeration string	64
viruscat	virus category	string	260
vulnid	id of the vulnerability	int	20
vulnname	name of the vulnerability	string	128
vulnseverity	severity level	string	8
vulncat	category	string	32
vulncvss	cvss score	string	64
vulnref	reference of the vulnerability	string	256
vulnengine	engine version	string	64

Log Field Name	Description	Data Type	Length
vulnsignature	signature version	string	260
vulnproducts	name of the vulnerable product	string	2048
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

systemevent

Log Field Name	Description	Data Type	Length
eponlinest	online status	enumeration string	32
epplace	EP place	enumeration string	32
emshostname	EMS host name	string	64
status	status description	string	16
emsip	EMS IP	string	20
fctip	FCT IP	string	20
epmgmtst	management status	enumeration string	64
epquarmsg	quarant message	string	260
epfeatures	installed features list	string	128
epenfeatures	enabled features list	string	128
ephbemsduration	EMS heart beat duration	int	20
ephbemslast	EMS heart beat last time	string	64
social_email	social email	string	128
social_phone	social phone number	string	64
social_srvc	social service	string	64
social_user	social user name	string	256
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32

Log Field Name	Description	Data Type	Length
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

Log message by type

securityevent > av

Log ID	Level	Sub Type	Event Type	Message
96530	warning	av	action	Found virus

Field	Field Description	Field Type
action	block or monitor	string
file	file location	string
virus	virus name	string
sigid	signature id	string
from	email from	string
to	email to	string
service	network protocol	string
vpn	vpn tunnel name	string

Log ID	Level	Sub Type	Event Type	Message

Field	Field Description	Field Type
filesize	file size	int
checksum	file crc32 checksum	int
detectedby	the security feature that detected virus	enumeration string
detectedin	where the virus is detected	enumeration string

Log ID	Level	Sub Type	Event Type	Message
96531	warning	av	warning	Found malware

Field	Field Description	Field Type
action	block or monitor	string
file	file location	string
virus	virus name	string
viruscat	virus category	string
sigid	signature id	string
filesize	file size	int
checksum	file crc32 checksum	int
detectedby	the security feature that detected virus	enumeration string
detectedin	where the virus is detected	enumeration string

securityevent > vulnerabilityscan

Log ID	Level	Sub Type	Event Type	Message
96521	info	vulnerabilityscan	status	A vulnerability scan result has been logged

Field	Field Description	Field Type
vulnid	id of the vulnerability	int
vulnname	name of the vulnerability	string
vulnseverity	severity level	string

Log ID	Level	Sub Type	Event Type	Message

Field	Field Description	Field Type
vulncat	category	string
vulncvss	cvss score	string
vulnref	reference of the vulnerability	string
vulnengine	engine version	string
vulnsignature	signature version	string
vulnproducts	name of the vulnerable product	string

Log ID	Level	Sub Type	Event Type	Message
96522	info	vulnerabilityscan	status	Applying patch for vulnerability found

Field	Field Description	Field Type
vulnid	id of the vulnerability	int
vulnname	name of the vulnerability	string
vulnseverity	severity level	string
vulncat	category	string
vulncvss	cvss score	string
vulnref	reference of the vulnerability	string
vulnengine	engine version	string
vulnsignature	signature version	string
vulnproducts	name of the vulnerable product	string

systemevent > endpoint

Log ID	Level	Sub Type	Event Type	Message
96953	info	endpoint	status	Endpoint Control Status Changed

Log ID	Level	Sub Type	Event Type	Message
				Field / **Field Description** / **Field Type** eponlinest / online status / enumeration string epplace / EP place / enumeration string emshostname / EMS host name / string status / status description / string
96955	info	endpoint	status	Endpoint Control Registration Status Changed
				Field / **Field Description** / **Field Type** emshostname / EMS host name / string status / status description / string emsip / EMS IP / string fctip / FCT IP / string
96956	info	endpoint	status	Endpoint Quarantine Status Changed
				Field / **Field Description** / **Field Type** epmgmtst / management status / enumeration string epquarmsg / quarant message / string emshostname / EMS host name / string
96957	info	endpoint	status	Endpoint Ext Log to FAZ
				Field / **Field Description** / **Field Type** epfeatures / installed features list / string epenfeatures / enabled features list / string ephbemsduration / EMS heart beat duration / int ephbemslast / EMS heart beat last time / string emshostname / EMS host name / string
96958	info	endpoint	status	User social media information

Log ID	Level	Sub Type	Event Type	Message

Field	Field Description	Field Type
social_email	social email	string
social_phone	social phone number	string
social_srvc	social service	string
social_user	social user name	string

Linux

This section contains the following information for FortiClient (Linux):

- Mandatory fields on page 15: fields that are mandatory to all FortiClient (Linux) logs.
- Log fields by type on page 16: fields that only apply to security event logs.
- Log message by type on page 19: lists each possible log message, sorted by log type and subtype.

Mandatory fields

Log Field Name	Description	Data Type
date	date	string
time	time	string
logver	log protocol version	int
id	log id	int
type	Traffic, Security Event or System Event	string
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string
eventtype	type of event	enumeration string
level	log level	enumeration string
uid	FortiClient unique ID	string
devid	device ID	string
hostname	host name of local machine	string
pcdomain	domain name of local machine	string
deviceip	device IP address	string
devicemac	device MAC address	string
vd	vdom	string
fctver	FCT version	string
fgtserial	FGT serial number	string
emsserial	EMS serial number	string
usingpolicy	current policy name	string

Log Field Name	Description	Data Type
os	operating system	string
user	current logged on user	string
msg	description of this log	string

Log fields by type

securityevent

Log Field Name	Description	Data Type	Length
action	block or monitor	string	32
file	file location	string	256
virus	virus name	string	512
sigid	signature id	string	260
from	email from	string	128
to	email to	string	512
service	network protocol	string	64
vpn	vpn tunnel name	string	32
filesize	file size	int	20
checksum	file crc32 checksum	int	20
detectedby	the security feature that detected virus	enumeration string	64
detectedin	where the virus is detected	enumeration string	64
viruscat	virus category	string	260
vulnid	id of the vulnerability	int	20
vulnname	name of the vulnerability	string	128
vulnseverity	severity level	string	8
vulncat	category	string	32
vulncvss	cvss score	string	64
vulnref	reference of the vulnerability	string	256
vulnengine	engine version	string	64

Log Field Name	Description	Data Type	Length
vulnsignature	signature version	string	260
vulnproducts	name of the vulnerable product	string	2048
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

systemevent

Log Field Name	Description	Data Type	Length
eponlinest	online status	enumeration string	32
epplace	EP place	enumeration string	32
emshostname	EMS host name	string	64
status	status description	string	16
emsip	EMS IP	string	20
fctip	FCT IP	string	20
epmgmtst	management status	enumeration string	64
epquarmsg	quarant message	string	260
epfeatures	installed features list	string	128
epenfeatures	enabled features list	string	128
ephbemsduration	EMS heart beat duration	int	20
ephbemslast	EMS heart beat last time	string	64
social_email	social email	string	128
social_phone	social phone number	string	64
social_srvc	social service	string	64
social_user	social user name	string	256
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32

Log Field Name	Description	Data Type	Length
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

Log message by type

securityevent > av

Log ID	Level	Sub Type	Event Type	Message
96530	warning	av	action	Found virus

Field	Field Description	Field Type
action	block or monitor	string
file	file location	string
virus	virus name	string
sigid	signature id	string
from	email from	string
to	email to	string
service	network protocol	string
vpn	vpn tunnel name	string

Log ID	Level	Sub Type	Event Type	Message

Field	Field Description	Field Type
filesize	file size	int
checksum	file crc32 checksum	int
detectedby	the security feature that detected virus	enumeration string
detectedin	where the virus is detected	enumeration string

Log ID	Level	Sub Type	Event Type	Message
96531	warning	av	warning	Found malware

Field	Field Description	Field Type
action	block or monitor	string
file	file location	string
virus	virus name	string
viruscat	virus category	string
sigid	signature id	string
filesize	file size	int
checksum	file crc32 checksum	int
detectedby	the security feature that detected virus	enumeration string
detectedin	where the virus is detected	enumeration string

securityevent > vulnerabilityscan

Log ID	Level	Sub Type	Event Type	Message
96521	info	vulnerabilityscan	status	A vulnerability scan result has been logged

Field	Field Description	Field Type
vulnid	id of the vulnerability	int
vulnname	name of the vulnerability	string
vulnseverity	severity level	string

Log ID	Level	Sub Type	Event Type	Message

Field	Field Description	Field Type
vulncat	category	string
vulncvss	cvss score	string
vulnref	reference of the vulnerability	string
vulnengine	engine version	string
vulnsignature	signature version	string
vulnproducts	name of the vulnerable product	string

Log ID	Level	Sub Type	Event Type	Message
96522	info	vulnerabilityscan	status	Applying patch for vulnerability found

Field	Field Description	Field Type
vulnid	id of the vulnerability	int
vulnname	name of the vulnerability	string
vulnseverity	severity level	string
vulncat	category	string
vulncvss	cvss score	string
vulnref	reference of the vulnerability	string
vulnengine	engine version	string
vulnsignature	signature version	string
vulnproducts	name of the vulnerable product	string

systemevent > endpoint

Log ID	Level	Sub Type	Event Type	Message
96953	info	endpoint	status	Endpoint Control Status Changed

Log ID	Level	Sub Type	Event Type	Message
				Field / **Field Description** / **Field Type** eponlinest / online status / enumeration string epplace / EP place / enumeration string emshostname / EMS host name / string status / status description / string
96955	info	endpoint	status	Endpoint Control Registration Status Changed
				Field / **Field Description** / **Field Type** emshostname / EMS host name / string status / status description / string emsip / EMS IP / string fctip / FCT IP / string
96956	info	endpoint	status	Endpoint Quarantine Status Changed
				Field / **Field Description** / **Field Type** epmgmtst / management status / enumeration string epquarmsg / quarant message / string emshostname / EMS host name / string
96957	info	endpoint	status	Endpoint Ext Log to FAZ
				Field / **Field Description** / **Field Type** epfeatures / installed features list / string epenfeatures / enabled features list / string ephbemsduration / EMS heart beat duration / int ephbemslast / EMS heart beat last time / string emshostname / EMS host name / string
96958	info	endpoint	status	User social media information

Log ID	Level	Sub Type	Event Type	Message

Field	Field Description	Field Type
social_email	social email	string
social_phone	social phone number	string
social_srvc	social service	string
social_user	social user name	string

www.fortinet.com